acm PORTAL
US Patent & Trademark Office

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

vmm platform emulation security

SEARCH

[redacted]

Feedback Report a problem Satisfaction survey

Terms used **vmm platform emulation security**

Found **5,494** of **147,060**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale □ ▁ ▃ ▆ ■

1 Virtual machines: ReVirt: enabling intrusion analysis through virtual-machine logging and replay ▆
George W. Dunlap, Samuel T. King, Sukru Cinar, Murtaza A. Basrai, Peter M. Chen
December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI
Full text available: pdf(1.56 MB) Additional Information: full citation, abstract, references, citings

Current system loggers have two problems: they depend on the integrity of the operating system being logged, and they do not save sufficient information to replay and analyze attacks that include any non-deterministic events. ReVirt removes the dependency on the target operating system by moving it into a virtual machine and logging below the virtual machine. This allows ReVirt to replay the system's execution before, during, and after an intruder compromises the system, even if the intruder rep ...

2 Virtual machine monitors: Terra: a virtual machine-based platform for trusted computing ▆
Tal Garfinkel, Ben Pfaff, Jim Chow, Mendel Rosenblum, Dan Boneh
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Full text available: pdf(140.31 KB) Additional Information: full citation, abstract, references, index terms

We present a flexible architecture for trusted computing, called Terra, that allows applications with a wide range of security requirements to run simultaneously on commodity hardware. Applications on Terra enjoy the semantics of running on a separate, dedicated, tamper-resistant hardware platform, while retaining the ability to run side-by-side with normal applications on a general-purpose computing platform. Terra achieves this synthesis by use of a *trusted virtual machine monitor* (TVMM ...

Keywords: VMM, attestation, authentication, trusted computing, virtual machine, virtual machine monitor

3 Virtualizing the VAX architecture ▆
Judith S. Hall, Paul T. Robinson

April 1991 **ACM SIGARCH Computer Architecture News , Proceedings of the 18th annual international symposium on Computer architecture,** Volume 19 Issue 3

Full text available: pdf(1.17 MB) Additional Information: full citation, references, citings, index terms

4 DRM usability and legal issues: On the implications of machine virtualization for DRM and fair use: a case study of a virtual audio device driver

Ninad Ghodke, Renato Figueiredo

October 2004 **Proceedings of the 4th ACM workshop on Digital rights management**

Full text available: pdf(328.01 KB) Additional Information: full citation, abstract, references, index terms

This paper examines the architecture of present day systems and shows that they are not trustworthy enough to support certain DRM features/restrictions, even when the DRM delivery system exclusively utilizes signed and protected operating system components. This weakness was discovered while creating a technique for remote transfer of audio streams generated by a Virtual Machine Monitor (VMM), to achieve network transparency for audio devices. The technique is based on the implementation of h ...

Keywords: digital rights management, virtual devices, virtual machines

5 Queue Focus: The Reincarnation of Virtual Machines

Mendel Rosenblum

July 2004 **Queue**, Volume 2 Issue 5

Full text available: pdf(853.72 KB) html(24.29 KB) Additional Information: full citation

6 Virtual machines: Scale and performance in the Denali isolation kernel

Andrew Whitaker, Marianne Shaw, Steven D. Gribble

December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI

Full text available: pdf(1.91 MB) Additional Information: full citation, abstract, references, citings

This paper describes the Denali isolation kernel, an operating system architecture that safely multiplexes a large number of untrusted Internet services on shared hardware. Denali's goal is to allow new Internet services to be "pushed" into third party infrastructure, relieving Internet service authors from the burden of acquiring and maintaining physical infrastructure. Our isolation kernel exposes a virtual machine abstraction, but unlike conventional virtual machine monitors, Denali does not ...

7 Reliability: Devirtualizable virtual machines enabling general, single-node, online maintenance

David E. Lowell, Yasushi Saito, Eileen J. Samberg

October 2004 **Proceedings f the 11th international c nference on Architectural support for programming languages and operating systems**

Full text available: pdf(174.01 KB) Additional Information: full citation, abstract, references, index terms

Maintenance is the dominant source of downtime at high availability sites. Unfortunately, the dominant mechanism for reducing this downtime, cluster rolling upgrade, has two shortcomings that have prevented its broad acceptance. First, cluster-style maintenance over many nodes is typically performed a few nodes at a time, mak-ing maintenance slow and often impractical. Second, cluster-style maintenance does not work on single-node systems, despite the fact that their unavailability during mainte ...

Keywords: availability, online maintenance, planned downtime, virtual machines

8 DAISY: dynamic compilation for 100% architectural compatibility
Kemal Ebcioğlu, Erik R. Altman
May 1997 **ACM SIGARCH Computer Architecture News , Proceedings of the 24th annual international symposium on Computer architecture,** Volume 25 Issue 2
Full text available: pdf(1.97 MB) Additional Information: full citation, abstract, references, citings, index terms

Although VLIW architectures offer the advantages of simplicity of design and high issue rates, a major impediment to their use is that they are not compatible with the existing software base. We describe new simple hardware features for a VLIW machine we call **DAISY** (**D***ynamically* **A***rchitected* **I***nstruction* **S***et from* **Y***orktown*). **DAISY** is specifically intended to emulate existing architectures, so that all existing softwa ...

Keywords: binary translation, dynamic compilation, instruction-level parallelism, object code compatible VLIW, superscalar

9 Virtual machine monitors: Xen and the art of virtualization
Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt, Andrew Warfield
October 2003 **Proceedings of the nineteenth ACM symposium on Operating systems principles**
Full text available: pdf(168.76 KB) Additional Information: full citation, abstract, references, citings, index terms

Numerous systems have been designed which use virtualization to subdivide the ample resources of a modern computer. Some require specialized hardware, or cannot support commodity operating systems. Some target 100% binary compatibility at the expense of performance. Others sacrifice security or functionality for speed. Few offer resource isolation or performance guarantees; most provide only best-effort provisioning, risking denial of service.This paper presents Xen, an x86 virtual machine monit ...

Keywords: hypervisors, paravirtualization, virtual machine monitors

10 A blueprint for introducing disruptive technology into the Internet
Larry Peterson, Tom Anderson, David Culler, Timothy Roscoe
January 2003 **ACM SIGCOMM Computer Communication Review,** Volume 33 Issue 1
Full text available: pdf(140.78 KB) Additional Information: full citation, abstract, references, index terms

This paper argues that a new class of geographically distributed network services is emerging, and that the most effective way to design, evaluate, and deploy these services is by using an overlay-based testbed. Unlike conventional network testbeds, however, we advocate an approach that supports both researchers that want to develop new services, and clients that want to use them. This dual use, in turn, suggests four design principles that are not widely supported in existing testbeds: services ...

11 Operating system: The persistent relevance of the local operating system to global applications
Jay Lepreau, Bryan Ford, Mike Hibler
September 1996 **Proceedings of the 7th workshop on ACM SIGOPS European workshop: Systems support for worldwide applications**
Full text available: pdf(828.93 KB) Additional Information: full citation, abstract, references, citings

The growth and popularity of loosely-coupled distributed systems such as the World Wide Web and the touting of Java-based systems as the solution to the issues of software maintenance, flexibility, and security are changing the research emphasis away from traditional single node operating system issues. Apparently, the view is that traditional OS issues are either solved problems or minor problems. By contrast, we believe that building such vast distributed systems upon the fragile infrastructur ...

12 Session summaries from the 17th symposium on operating systems principle (SOSP'99)
Jay Lepreau, Eric Eide
April 2000 **ACM SIGOPS Operating Systems Review**, Volume 34 Issue 2
Full text available: pdf(3.15 MB) Additional Information: full citation, index terms

13 Development of processors and communication networks for embedded systems: System design methodologies for a wireless security processing platform
Srivaths Ravi, Anand Raghunathan, Nachiketh Potlapally, Murugan Sankaradass
June 2002 **Proceedings of the 39th conference on Design automation**
Full text available: pdf(207.37 KB) Additional Information: full citation, abstract, references, citings, index terms

Security protocols are critical to enabling the growth of a wide range of wireless data services and applications. However, they impose a high computational burden that is mismatched with the modest processing capabilities and battery resources available on wireless clients. Bridging the security processing gap, while retaining sufficient programmability in order to support a wide range of current and future security protocol standards, requires the use of novel system architectures and design m ...

Keywords: 3DES, AES, DES, IPSec, RSA, SSL, decryption, design methodology, embedded system, encryption, handset, performance, platform, security, security processing, system architecture, wireless

14 Cellular disco: resource management using virtual clusters on shared-memory multiprocessors
Kinshuk Govil, Dan Teodosiu, Yongqiang Huang, Mendel Rosenblum

August 2000 **ACM Transacti ns on C mputer Systems (TOCS)**, Volume 18 Issue 3

Full text available: pdf(287.05 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Despite the fact that large-scale shared-memory multiprocessors have been commercially available for several years, system software that fully utilizes all their features is still not available, mostly due to the complexity and cost of making the required changes to the operating system. A recently proposed approach, called Disco, substantially reduces this development cost by using a virtual machine monitor that laverages the existing operating system technology. In this paper we present a ...

Keywords: fault containment, resource managment, scalable multiprocessors, virtual machines

15 Application performance and flexibility on exokernel systems

M. Frans Kaashoek, Dawson R. Engler, Gregory R. Ganger, Héctor M. Briceño, Russell Hunt, David Mazières, Thomas Pinckney, Robert Grimm, John Jannotti, Kenneth Mackenzie

October 1997 **ACM SIGOPS Operating Systems Review , Proceedings of the sixteenth ACM symposium on Operating systems principles,** Volume 31 Issue 5

Full text available: pdf(2.39 MB) Additional Information: full citation, references, citings, index terms

16 Cellular Disco: resource management using virtual clusters on shared-memory multiprocessors

Kinshuk Govil, Dan Teodosiu, Yongqiang Huang, Mendel Rosenblum

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles,** Volume 33 Issue 5

Full text available: pdf(1.93 MB) Additional Information: full citation, abstract, references, citings, index terms

Despite the fact that large-scale shared-memory multiprocessors have been commercially available for several years, system software that fully utilizes all their features is still not available, mostly due to the complexity and cost of making the required changes to the operating system. A recently proposed approach, called Disco, substantially reduces this development cost by using a virtual machine monitor that leverages the existing operating system technology.In this paper we present a syste ...

17 Intrusion detection: Randomized instruction set emulation to disrupt binary code injection attacks

Elena Gabriela Barrantes, David H. Ackley, Trek S. Palmer, Darko Stefanovic, Dino Dai Zovi

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security**

Full text available: pdf(160.71 KB) Additional Information: full citation, abstract, references, citings, index terms

Binary code injection into an executing program is a common form of attack. Most current defenses against this form of attack use a 'guard all doors' strategy, trying to block the avenues by which execution can be diverted. We describe a complementary method of protection, which disrupts foreign code execution regardless of how the code is injected. A unique and private machine instruction set for each executing program would make it difficult for an outsider to design binary attack code against ...

Keywords: automated diversity, emulation, information hiding, language randomization, obfuscation, security

18 The DGSA: unmet information security challenges for operating system designers
Edward A. Feustel, Terry Mayfield
January 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 1
Full text available: pdf(1.48 MB) Additional Information: full citation, abstract, citings, index terms

The Department of Defense (DoD) Goal Security Architecture (DGSA) introduces a broader view of information security from that previously held by the Department, one which has much more in common with the requirements of an inter-networked commercial view of information security. The purpose of this paper is to introduce designers of operating systems to the most important aspects of the DGSA conceptual framework in order to open discussions on both the suitability of the framework and the feasib ...

19 Operating systems security: Attestation-based policy enforcement for remote access
Reiner Sailer, Trent Jaeger, Xiaolan Zhang, Leendert van Doorn
October 2004 **Proceedings of the 11th ACM conference on Computer and communications security**
Full text available: pdf(261.52 KB) Additional Information: full citation, abstract, references, index terms

Intranet access has become an essential function for corporate users. At the same time, corporation's security administrators have little ability to control access to corporate data once it is released to remote clients. At present, no confidentiality or integrity guarantees about the remote access clients are made, so it is possible that an attacker may have compromised a client process and is now downloading or modifying corporate data. Even though we have corporate-wide access control over ...

Keywords: remote access, security management, trusted computing

20 Data integrity: Web application security assessment by fault injection and behavior monitoring
Yao-Wen Huang, Shih-Kun Huang, Tsung-Po Lin, Chung-Hung Tsai
May 2003 **Proceedings of the twelfth international conference on World Wide Web**
Full text available: pdf(4.53 MB) Additional Information: full citation, abstract, references, citings, index terms

As a large and complex application platform, the World Wide Web is capable of delivering a broad range of sophisticated applications. However, many Web applications go through rapid development phases with extremely short turnaround time, making it difficult to eliminate vulnerabilities. Here we analyze the design of Web application security assessment mechanisms in order to identify poor coding practices that render Web applications vulnerable to attacks such as SQL injection and cross-site scr ...

Keywords: black-box testing, complete crawling, fault injection, security assessment, web application testing

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Welcome
United States Patent and Trademark Office

IEEE Xplore® 1 Million Documents 1 Million Users ...And Growing

Help FAQ Terms IEEE Peer Review

Quick Links

» Search Results

Welcome to IEEE Xplore®
- Home
- What Can I Access?
- Log-out

Tables of Contents
- Journals & Magazines
- Conference Proceedings
- Standards

Search
- By Author
- Basic
- Advanced
- CrossRef

Member Services
- Join IEEE
- Establish IEEE Web Account
- Access the IEEE Member Digital Library

IEEE Enterprise
- Access the IEEE Enterprise File Cabinet

Your search matched **2** of **1099723** documents.
A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance** in **Descending** order.

Refine This Search:
You may refine your search by editing the current search expression or entering a new one in the text box.

arbaugh<and>farber<and>smith Search

□ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

1 **Security for virtual private intranets**
Arbaugh, W.A.; Davin, J.R.; Farber, D.J.; Smith, J.M.;
Computer , Volume: 31 , Issue: 9 , Sept. 1998
Pages:48 - 55

[Abstract] [PDF Full-Text (236 KB)] **IEEE JNL**

2 **A secure and reliable bootstrap architecture**
Arbaugh, W.A.; Farber, D.J.; Smith, J.M.;
Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on , 4-7 May 1997
Pages:65 - 71

[Abstract] [PDF Full-Text (600 KB)] **IEEE CNF**